



Precinct Voting Denial of Service

Prepared for NIST “Threats to Voting Systems” Workshop

**R. Michael Alvarez
Caltech/MIT Voting Technology Project
October 5, 2005**

This is a type of threat that has a long history in electoral politics, and can take many forms.¹ The basic approach is that a perpetrator attacks precinct voting, regardless of voting system, on election day in an effort to disrupt the process sufficiently to produce an effective “denial of service” attack. The perpetrator, based on an analysis of past elections returns, would target selected precincts that are highly likely to cast votes in a certain direction. For example, if the perpetrator wished to sway the election for party X, he or she would target precincts that have very heavy concentrations of party Y supporters. In a close election, especially in lower-level races, such an attack could either sway the outcome of an election to party X or could throw considerable doubt and distrust into the announced election outcome.

Such an attack could be mounted in a wide variety of ways. The perpetrator could attempt to mount some sort of disturbance at certain critical times on election day in selected precincts. For example, in a high-turnout election where there are long lines of citizens waiting to vote just before polls close, the perpetrator could stage a protest at the entrance of the poll site; while such a demonstration is likely to be illegal if sufficiently close to the polling place, again if it either led some number of citizens to turn away and

¹ Benseal writes about political clubs in Baltimore during the 1850’s, and he described one example of this threat: “The usual tactics used by these clubs on election day entailed the occupation of the area in front of the voting window by dozens of their members. Would-be voters were then forced to make their way through the crowd in order to hand their tickets to the election judges. As they moved through the crowd, club members would insist on seeing the ticket they wished to vote. If it was the American ticket, the crowd would part ranks, making an open path to the window. If it was the Democratic or “reform” ticket (a euphemism for the Democratic ticket), a cry would go out, alerting other club members that a member of the opposition was attempting to vote ... This was the signal prompting a general movement of the members in mass, outward to the street. The would-be voter was thus physically moved away from the window by the sheer bulk of the crowd” (Richard Franklin Benseal, *The American Ballot Box in the Mid-Nineteenth Century*, Cambridge University Press, 2000, pages 171-172).

not vote, or led to the perception that some number of citizens were not allowed to vote, many might question the integrity of the election.² Or, the perpetrator could coordinate sending confederates to certain polling places to intimidate potential voters, similar to the historical example cited above.³

Other ways such an attack could be mounted might be more difficult to monitor and prevent. For example, the perpetrator could threaten the operation of the polling place by sending operatives to somehow disable or cripple the voting devices (or a sufficiently large subset of the voting devices to generate confusion and long lines) early on election day, thus leading to long lines and potential disenfranchisement of voters later in the day. Or they could disable or cripple the voting devices near the close of voting on election day, producing long lines and potentially disenfranchising voters who might be told they were not allowed to vote after the close of the polls (or who grew frustrated and leave). The method of such an attack would depend on the voting system in place, and the perpetrator's ability to coordinate a number of confederates to assist in the attack.

Such attacks could be mounted as insider attacks. For example, in 2002 the U.S. Department of Justice resolved voting rights complaints in two Florida counties; the complaints alleged that one county "had not translated all of its election documents and information into Spanish, failed to assign a sufficient number of bilingual poll officials to polling sites with significant numbers of Spanish-speaking voters, and denied some voters assistance from persons of their own choosing."⁴ If the perpetrator were able to recruit conspirators to assist in such denial-of-service attacks in such ways, such attacks could be mounted and could be difficult to prevent on election day, or even in the immediate aftermath of the election. They could result in considerable voter disenfranchisement, and could again cast doubt on the integrity of the election outcome.

Of course, such an attack could be mounted in a much more coordinated way, by a highly motivated and well-resourced perpetrator. For example, a highly-motivated and well-resourced perpetrator could attack infrastructure on election day, in a number of ways that either could directly disrupt the voting process or which could indirectly serve to distract or disenfranchise voters in certain areas of a jurisdiction. A perpetrator in such a scenario could disrupt utility service to some targeted part of an election jurisdiction (again the perpetrator could attack utility service in a part of the jurisdiction that has a high concentration of party Y supporters, thereby distracting or disenfranchising such

² While laws exist to help prevent direct voter intimidation or electioneering close to the entrance to polling places, one could imagine that a sufficiently large public demonstration near a polling place could serve as a distraction or effectively block access to the polling place, disrupting service for otherwise eligible voters at that polling place, for example, by blocking access to parking lots or by making access difficult from local surface streets.

³ For modern allegations of voter intimidation tactics, see the report from the People For The American Way Foundation, "The Long Shadow of Jim Crow", http://www.pfaw.org/pfaw/dfiles/file_462.pdf (last touched October 5, 2005).

⁴ See http://www.usdoj.gov/opa/pr/2002/February/02_crt_380.htm for details of the allegations and the consent decree.

voters if the attack prevents or distracts them from voting), or across a series of election jurisdictions.⁵

Also, perpetrators could mount highly effective denial-of-service attacks on election day in precinct voting if they could mount successful pre-election attacks (either insider or by other means) on election administration systems. An example here would be a pre-election attack on a voter registration file (either at the local or state level). The perpetrator, with access to an electronic voter registration file with associated voter history data could effectively disenfranchise certain types of voters (say again those highly likely to cast ballots for their opponent, determined from either their partisan registration or voting history information) by altering their registration status, changing registration information, or perhaps altering records like early or absentee voting status in the current election. Eligible voters showing up to vote in the affected precincts would find their names not on the voter registration list, or be told they had already voted, either directly disenfranchising those voters or causing significant disruptions and long lines.

The resources needed to mount these attacks vary with their planned scope. In closely contested local elections, the perpetrator might need to effectively disrupt polling place operations in a single precinct, if their opponent's supporters are highly concentrated in that precinct, to potentially keep even a handful of the opposition's supporters from having the opportunity to vote. Effective denial of service attacks, mounted in different elections (say legislative races) would require more resources, primarily requiring that the perpetrator recruit and coordinate the activities of a greater number of confederates. Or, a well-resourced perpetrator could attempt a denial-of-service attack, as noted above, without many confederates by targeting infrastructure.

As noted a number of times, these attacks can have two consequences. One direct consequence is the disenfranchisement of a selected set of targeted voters, who have been prevented or discouraged from voting. An indirect consequence is doubts raised about the integrity of the election outcome. There are some mitigation strategies for the direct effect, including extending polling hours, allowing impacted voters the right to quickly and easily cast provisional ballots in another polling place, or in the case of a broad attack, holding another election.⁶ The most problematic aspect of any denial-of-service attack, however, is the threat to the integrity of an election. Thus, even low-level denial-of-service attacks, occurring in a hotly contested election, might pose a substantial risk.

⁵ Some of these scenarios have been explored by John C. Fortier and Norman J. Ornstein, in their *Election Law Journal*, "If Terrorists Attacked Our Presidential Elections" (Volume 3, Number 4, 2004, pages 597-612.). See especially the section "The Disruption of Election Day", pages 601-604.

⁶ These mitigation strategies might be ones that some election officials may have planned for, but in the context of natural disasters. However, if some type of denial of service attack were undertaken that affected a number of election jurisdictions, it might be difficult to quickly coordinate a response on election day that might alleviate potential voter disenfranchisement.